Purva Rumde

Small Business Phishing Prevention Policy

This Phishing Prevention Policy establishes security measures to protect small businesses from phishing attacks by implementing email security controls, employee training, incident response procedures, and technical defenses in alignment with ISO 27001, NIST CSF, and CIS Controls.

Table of Contents

1. Introduction

1.1 Purpose

This policy establishes security measures to protect the small business from phishing attacks, a common cyber threat that exploits human vulnerabilities. It aligns with ISO 27001, NIST Cybersecurity Framework (CSF), and CIS Controls.

1.2 Scope

This policy applies to all employees, contractors, and third-party vendors who access company email, communication systems, and sensitive data.

2. Roles and Responsibilities

2.1 Management

- Responsible for enforcing anti-phishing policies and ensuring compliance.
- Approves cybersecurity awareness training initiatives.
- Encourages a culture of cybersecurity vigilance within the organization.

2.2 IT Team/Security Officer

- Implements **email filtering and anti-phishing solutions**.
- Monitors phishing attempts and provides regular reports.
- Responds to phishing incidents and coordinates remediation efforts.

2.3 Employees

- Complete **phishing awareness training**.
- Report suspicious emails to IT/security personnel.
- Follow best practices for **email security and verification**.

3. Phishing Prevention Controls

3.1 Email Security Measures

- Enable **email filtering systems** to detect phishing attempts.
- Implement **DMARC, DKIM, and SPF** email authentication protocols.
- Block emails from known phishing domains and IP addresses.
- Restrict **clickable links** in external emails unless verified.

3.2 Employee Awareness & Training

- Conduct **mandatory phishing awareness training** upon hiring and annually.
- Perform **quarterly phishing simulation tests**.
- Teach employees how to **identify phishing red flags**, such as:
    - Unusual sender addresses.
    - Urgent requests for sensitive information.
    - Unexpected email attachments or links.

3.3 Incident Response for Phishing Attacks

- Employees must report suspected phishing emails immediately to IT/security.
- IT Team should **quarantine and analyze** the reported email.
- If credentials were compromised, **force password resets** and notify affected users.
- Document incidents for continuous improvement and security enhancement.

3.4 Technical Security Controls

- Enforce **Multi-Factor Authentication (MFA)** on all business-critical accounts.
- Implement **Endpoint Detection and Response (EDR)** solutions.
- Monitor **network traffic** for indicators of phishing-based malware.
- Enable **automatic software updates** to patch vulnerabilities.

4. Compliance & Review

4.1 Compliance Requirements

- This policy ensures compliance with **ISO 27001, NIST CSF, and CIS Controls**.
- Regular **audits of phishing prevention measures** should be conducted.
- Employees must acknowledge and adhere to phishing prevention guidelines.

4.2 Policy Review Process

- This policy must be reviewed **annually or after any significant phishing attack**.
- Updates should be documented and approved by senior management.
- Feedback from phishing simulations should be used to enhance training materials.

5. Glossary & References

5.1 Glossary

- **Phishing**: A cyber-attack where attackers impersonate legitimate sources to steal sensitive information.
- **DMARC, DKIM, SPF**: Email authentication protocols that verify sender legitimacy.
- **Multi-Factor Authentication (MFA)**: Security requiring multiple verification steps.
- **Endpoint Detection and Response (EDR)**: Advanced security solutions that detect and mitigate cyber threats on devices.

5.2 References

- ISO/IEC 27001:2022 Information Security Management
- NIST Cybersecurity Framework (CSF)
- Center for Internet Security (CIS) Critical Security Controls
- Anti-Phishing Working Group (APWG) Best Practices